UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/600,856	06/19/2003	Kirby L. Kuehl	CSCO-6886	8485

20575   7590   10/02/2007

MARGER JOHNSON & MCCOLLOM, P.C.
210 SW MORRISON STREET, SUITE 400
PORTLAND, OR 97204

EXAMINER
PATEL, CHIRAG R

ART UNIT	PAPER NUMBER
2141	

MAIL DATE	DELIVERY MODE
10/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

	Application No.	Applicant(s)
Office Action Summary	10/600,856	KUEHL ET AL.
	Examiner	Art Unit	
	Chirag R. Patel	2141	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>24 September 2007</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>4-35 and 42-45</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) <u>4-12</u> is/are allowed.

6)☒ Claim(s) <u>13-35, 42-45</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

Response to Amendment

Applicant's request for reconsideration of the finality of the rejection of the last

Office action is persuasive and, therefore, the finality of that action is withdrawn.

Examiner notes that claims 1-3 and 36-42 are cancelled by the applicants.

Response to Arguments

Applicant's arguments filed September 24, 2007 have been fully considered but

they are not persuasive. A discussion is provided below.

As per claim 13, Billhartz discloses per Col 4 lines 4-13, "monitoring

transmissions among the plurality of nodes to detect service set IDs associated

therewith, and generating an intrusion alert based upon one of the detected service set

IDs being different than the at least one service set ID of the MANET." The detected

service set IDs is interpreted as the node that corresponds to the tracked entity. The

service set ID of the MANET is interpreted as the existing entry in database. The

detected service set ID of the transmitted mode is linked with the service set ID of the

MANET to assist in determining the conditions when the intrusion alarm will be

generated.

Billhartz discloses further per (Col 11 lines 5-11), "It will also be appreciated that

the above-described invention may be implemented in several ways. For example, the

policing node 13 could be implemented in one or more separate, dedicated devices that

are not already part of the MANET 10. Alternately, the invention may be implemented in

software to be installed on one or more existing nodes in a MANET where intrusion

detection is desired."

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 13-35, and 43 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Billhartz (US 6,986,161) in view of Ammon et al. – hereinafter Ammon (US

2003/0217289).

As per claims 13 and 25, Billhartz discloses an apparatus comprising:

one or more processors; and (Col 5 lines 49-60)

a memory coupled to the processors comprising instructions executable by the

processors, the processors operable when executing the instructions to: (Col 5 lines 49-

60, Col 11 lines 5-11)

receive node information for a node coupled to a computer network; (Col 4 lines

4-13)

analyze identifiers included in the received node information to select a value for

comparing to a database that lists tracked entities; (Col 4 lines 4-13)

determining whether the node corresponds to one of the tracked entities by

comparing the selected value to the database; (Col 4 lines 4-13)

when the node corresponds to one of the tracked entities, linking at least a

portion of the received node information to an existing entry in the database; and (Col 4

lines 4-13)

Billhartz fails to disclose when the node does not correspond to one of the

tracked entities, adding an entry for a new entity to the database and linking the node

information to the new entity. Ammon discloses when the node does not correspond to

one of the tracked entities, adding an entry for a new entity to the database and linking

the node information to the new entity. ([0023]) At the time the invention was made, it

would have been obvious to a person of ordinary skill in the art to disclose when the

node does not correspond to one of the tracked entities, adding an entry for a new entity

to the database and linking the node information to the new entity in the disclosure of

Billhartz. The motivation for doing do would have been to discover both authorized and

unauthorized access points and authorized and unauthorized client machines that may

be trying to connect to the wireless network. ([0023])

As per claim 14, Billhartz / Aamon disclose the apparatus of claim 13. Billhartz

discloses wherein the selected value is not based on an Internet Protocol (IP) address

such that the node can be correlated to one of the tracked entities. (Col 11 lines 12-22)

Billhartz fails to disclose wherein the selected value is not based on an Internet Protocol

(IP) address such that the node can be correlated to one of the tracked entities when

the node is subject to dynamic IP address assignment. ([0161] At the time the

invention was made, it would have been obvious to a person of ordinary skill in the art to

disclose wherein the selected value is not based on an Internet Protocol (IP) address

such that the node can be correlated to one of the tracked entities when the node is

subject to dynamic IP address assignment in the disclosure of Billhartz. The motivation

for doing do would have been to store the results of that monitoring, processes the

results to determine whether any unauthorized access of the wireless network of

interest has occurred, and notifies users of the results and the processing. ([0012])

As per claim 15, Billhartz/ Aamon disclose the apparatus of claim 13, and Billhartz

discloses wherein the selected value is based on a physical address for the node when

a security identifier is unavailable. (Col 6 lines 5-16; security identifier is unavailable in

this case)

As per claim 16, Billhartz / Aamon disclose the apparatus of claim 13, and

Billhartz discloses wherein the selected value is based on a physical address for the

node when a serial number is unavailable. (Col 6 lines 5-16; serial number is

unavailable in this case)

As per claim 17, Billhartz / Aamon disclose the apparatus of claim 13, and

Billhartz discloses wherein the selected value is based on a physical address for the

node when a different preferred identifier is unavailable. (Col 6 lines 5-16; different

preferred identifier is unavailable in this case)

As per claim 18, Billhartz / Aamon disclose the apparatus of claim 13, and

Billhartz discloses wherein the selected value is based on both a physical address and

a network address when a different preferred identifier is unavailable. (Col 6 lines 5-16;

different preferred identifier is unavailable in this case,   the remaining layers of the OSI

model may also be used for data transmission as well, and other suitable network data

transfer models may also be used , and that includes the network layer for IP or network

address)

As per claim 19, Billhartz / Aamon disclose the apparatus of claim 13, wherein the

selected value is a combination of the network address and a globally unique identifier.

(Col 6 lines 5-16)

As per claim 20, Billhartz/ Aamon disclose the apparatus of claim 13, and

Billhartz discloses the selected value is not based on an IPv4 address such the node

can be correlated to one of the tracked entities. (Col 6 line 5-16; based on MAC

address) Billhartz fails to disclose the selected value is not based on an IPv4 address

such the node can be correlated to one of the tracked entities even when the node is

subject to dynamic IPv4 address assignment. Aamon disclose the selected value is not

based on an IPv4 address such the node can be correlated to one of the tracked

entities even when the node is subject to dynamic IPv4 address assignment. ([0161])

At the time the invention was made, it would have been obvious to a person of ordinary

skill in the art to disclose the selected value is not based on an IPv4 address such the

node can be correlated to one of the tracked entities even when the node is subject to

dynamic IPv4 address assignment. The motivation for doing do would have been to

store the results of that monitoring, processes the results to determine whether any

unauthorized access of the wireless network of interest has occurred, and notifies users

of the results and the processing. ([0012])

As per claim 21, Billhartz/ Aamon disclose the apparatus of claim 13. Billhartz

discloses wherein the processors are further operable to:

select either a security identifier provided by an operating system of the node or

a serial number provided by a basic input output system of the node for the value when

the received node information includes either the security identifier or the serial number;

(Col 3 lines 10-22)

and select a physical address for the value when the received node information

does not include either the security identifier or the serial number. (Col 6 lines 5-16;

security identifier or serial identifier is unavailable in this case)

As per claim 22, Billhartz/ Aamon disclose the apparatus of claim 13. Billhartz

discloses wherein the processors are further operable to trigger issuance of an intrusion

alarm when the node does not correspond to one of the tracked entities. (Col 4 lines 4-

13)

As per claim 23, Billhartz/ Aamon disclose the apparatus of claim 13. Billhartz

discloses wherein issuance of a false alarm is avoided when the received node

information is linked to an existing entry in the database. (Col 4 lines 4-13)

As per claim 24, Billhartz / Aamon disclose the apparatus of claim 13. Billhartz

discloses wherein the processors are further operable to use adaptive scanning before

determining whether to issue an alarm. (Col 4 lines 4-13)

As per claim 26, Billhartz / Aamon disclose the system of claim 25. Billhartz

discloses wherein said multiple identifiers comprise a media access control (MAC)

address (Col 6 line 5-16)

As per claim 27, Billhartz/ Aamon disclose the system of claim 25. Billhartz

disclose wherein said multiple identifiers further comprise a computer name.   (Col 3

lines 10-22)

As per claim 28, Billhartz/ Aamon disclose the system of claim 27. Billhartz

discloses wherein said multiple identifiers further comprise a domain name. (Col 11

lines 12-22; authorized network as domain name)

As per claim 29, Billhartz / Aamon disclose the system of claim 28. Billhartz fails

to disclose wherein said multiple identifiers further comprise an operating system

identifier. Aamon discloses wherein said multiple identifiers further comprise an

operating system identifier. ([0055]) At the time the invention was made, it would have

been obvious to a person of ordinary skill in the art to disclose wherein said herein said

multiple identifiers further comprise an operating system identifier. The motivation for

doing do would have been to store the results of that monitoring, processes the results

to determine whether any unauthorized access of the wireless network of interest has

occurred, and notifies users of the results and the processing. ([0012])

As per claim 30, Billhartz/ Aamon disclose the system of claim 28. Billhartz

disclose wherein said multiple identifiers comprise at least two of: a media access

control (MAC) address, a computer name, a domain name, and an operating system

identifier. (Col 11 lines 12-22, authorized network as domain name)

As per claim 31, Billhartz/ Aamon disclose the system of claim 25. Billhartz

discloses wherein said unique identifier comprises a security identifier. (Col 3 lines 10-

22)

As per claim 32, Billhartz / Aamon disclose the system of claim 25. Billhartz fails

to disclose wherein said unique identifier comprises a serial number. Aamon discloses

wherein said unique identifier comprises a serial number. ([0117]-[0118]) At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to disclose wherein the other value is a security identifier, a serial number or a

physical address in the disclosure of Ammon. The motivation for doing do would have

been to store the results of that monitoring, processes the results to determine whether

any unauthorized access of the wireless network of interest has occurred, and notifies

users of the results and the processing. ([0012])

As per claim 33, Billhartz/ Aamon disclose the system of claim 25. Billhartz

discloses further comprising: returning an identifier for an entity in response to a request

including a node identifier. (Col 1 lines 38-52)

As per claim 34, Billhartz/ Aamon disclose the system of claim 25. Billhartz

discloses further comprising: means for returning identifiers for all nodes associated

with an entity in response to a request including an entity identifier. (Col 4 lines 4-13)

As per claim 35, Billhartz/ Aamon disclose the system of claim 25. Billhartz

discloses further comprising: means for returning node information in response to a

request for said node information including a node identifier. (Col 4 lines 4-13)

As per claim 43, Billhartz/Aamon disclose the same limitations as claim 1, and Billhartz further discloses wherein said engine is further operable to determine if a media access control (MAC) address from said node information matches a MAC address in said database, if there is not a unique identifier in said node information. (Col 4 lines 4-13, Col 6 lines 5-16)

Claims 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Billhartz (US 6,986,161) / Ammon (US 2003/0217289) further in view of Short et al. – hereinafter Short (US 7,194,554)

As per claim 44, Billhartz/Aamon disclose the system for tracking entities in a computer network of Claim 36. Billhartz fails to disclose further comprising means for determining if a computer name from said node information matches a computer name associated with said MAC address in said database. Short discloses further comprising means for determining if a computer name from said node information matches a computer name associated with said MAC address in said database. (Col 9 lines 8-26; Col 10 lines 9-37) At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to disclose further comprising means for determining if a computer name from said node information matches a computer name associated with said MAC address in said database in the disclosure of Billhartz. The motivation for doing do would have been to for selectively implementing and

enforcing Authentication, Authorization and Accounting (AAA) of users accessing a

network via a gateway device. (Col 3 lines 9-44)

As per claim 45, Billhartz/Aamon disclose the system for tracking entities in a

computer network of claim 36. Billhartz fails to disclose means for determining if a

computer name from said node information matches a computer name in said

database; and means for determining if a domain name from said node information

matches a domain name associated with said computer name in said database. Short

discloses means for determining if a computer name from said node information

matches a computer name in said database; and means for determining if a domain

name from said node information matches a domain name associated with said

computer name in said database. (Col 9 lines 8-26; Col 10 lines 9-37)   At the time

the invention was made, it would have been obvious to a person of ordinary skill in the

art to disclose means for determining if a computer name from said node information

matches a computer name in said database; and means for determining if a domain

name from said node information matches a domain name associated with said

computer name in said database in the disclosure of Billhartz. The motivation for doing

do would have been to for selectively implementing and enforcing Authentication,

Authorization and Accounting (AAA) of users accessing a network via a gateway device.

(Col 3 lines 9-44)

Allowable Subject Matter

Claims 4-8, and 9-12 are allowed.

The following is a statement of reasons for the indication of allowable subject matter: As per claim 4, Billhartz was relied upon per Col 2 lines 25-30, "provide a mobile ad-hoc network (MANET) with intrusion detection features and related methods." Ammon was relied upon to disclose per [0118], "This process checks the new IDS events and adds new unknown clients to the database according to the above schema. Information about the unknown clients that is entered into the database can include the MAC address, SSID, IP address, channel, signal strength, and WEP status"

As per claims 4 and 9, a thorough review of prior art fails to disclose specific conditions of "selecting a security identifier provided by an operating system of the node as the unique identifier when the analysis indicates that the node information includes the security identifier; selecting a serial number provided by a basic input output system of the node as the unique identifier when the analysis indicates that the node information does not include the security identifier; and selecting a physical address as the unique identifier when the analysis indicates that the node information does not include either of the security identifier and the serial number."

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chirag R Patel whose telephone number is (571)272-7966. The examiner can normally be reached on Monday to Friday from 7:30AM to 4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia, can be reached on (571) 272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pairdirect.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll free).

Chirag Patel
Patent Examiner

AU 2141

C.P. *C.P.*

JASON CARDONE
SUPERVISORY PATENT EXAMINER